

日 本 国 特 許 庁
JAPAN PATENT OFFICE

11017 U.S. PRO
10/087807
03/05/02

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application: 2001年 3月13日

出 願 番 号

Application Number: 特願2001-071214

[ST.10/C]:

[JP2001-071214]

出 願 人

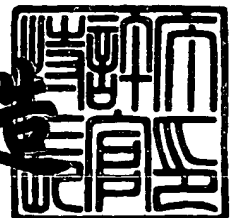
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 1月18日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3117349

【書類名】 特許願

【整理番号】 0150025

【提出日】 平成13年 3月13日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00
G06F 13/00

【発明の名称】 フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【請求項の数】 9

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 三友 仁史

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 鳥居 悟

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小谷 誠剛

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 滝沢 文恵

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 小野 越夫

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通
株式会社内

【氏名】 小谷野 修

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100089118

【弁理士】

【氏名又は名称】 酒井 宏明

【手数料の表示】

【予納台帳番号】 036711

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9717671

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 フィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラム

【特許請求の範囲】

【請求項 1】 クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積手段と、

前記見積手段による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定手段と、

を備えたことを特徴とするフィルタリング装置。

【請求項 2】 前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定手段は、前記見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする請求項 1 に記載のフィルタリング装置。

【請求項 3】 前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定手段は、前記見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする請求項 1 に記載のフィルタリング装置。

【請求項 4】 前記サーバに対する正当アクセスのパターンを格納した正当

パターンデータベースと、前記見積手段による正当性を見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする請求項 1、2 または 3 に記載のフィルタリング装置。

【請求項 5】 所定の外部送信ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信手段をさらに備えたことを特徴とする請求項 1～4 のいずれか一つに記載のフィルタリング装置。

【請求項 6】 所定の格納ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納手段をさらに備えたことを特徴とする請求項 1～5 のいずれか一つに記載のフィルタリング装置。

【請求項 7】 所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新手段をさらに備えたことを特徴とする請求項 1～6 のいずれか一つに記載のフィルタリング装置。

【請求項 8】 クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス要求のみを受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

を含んだことを特徴とするフィルタリング方法。

【請求項 9】 クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス

要求のみを受け渡すフィルタリング方法をコンピュータに実行させるプログラムにおいて、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

をコンピュータに実行させるプログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

この発明は、クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムに関する。

【 0 0 0 2 】

近時、ネットワーク技術の進展に伴って、インターネット上の分散システムであるWWW (World Wide Web) の利用が急速に拡大し、クライアントからの各種のリクエスト (アクセス要求) に応じて各種のサービスを提供する各種HTTPサーバも累増してきたが、かかるサーバの累増にともなって、クライアントによるサーバへの不正アクセスも増加しつつある。

【 0 0 0 3 】

すなわち、侵入者 (イントルーダ) や攻撃者 (アタッカ) が企業、団体、個人などのサーバを無権限で不正に利用したり、運用を妨害したり、破壊 (クラック) など、サーバを利用する者がその者に与えられた権限により許された行為以外の行為をネットワークを介して意図的におこなうという不正アクセスが増加している。このため、サーバに対する不正アクセスを拒絶することによりサーバの信頼性を確保する必要性が高まりつつある。

【 0 0 0 4 】

【従来の技術】

従来より、クライアントによる不正アクセスからサーバを守るために、インターネットと企業LAN (Local Area Network) との間にファイアウォール (Fire Wall) を構築することが一般的におこなわれている。

【0005】

このファイアウォールは、インターネットに接続したコンピューターやネットワークへの外部からの侵入を防ぐためのソフトウェアであり、企業LANとインターネットの間に、特定のデータやプロトコルだけを通すように設計されたファイアウォール用のコンピュータを置き、LAN内と外部とのデータ交換はすべてこのマシンを通しておこなうことにより、外部からの侵入を防ぐというものである。

【0006】

また、このファイアウォールに関連して、ネットワークベースあるいはホストベースの不正アクセス検知手法がある。前者のネットワークベースの不正アクセス検知手法は、ネットワークを流れる生のパケットを監視することにより不正アクセスを発見するものであり、後者のホストベースの不正アクセス検知手法は、ホストに蓄えられたログ履歴を監視することにより不正アクセスを発見するものである。

【0007】

そして、このような不正アクセス検知手法により発見された不正アクセスに基づいて不正アクセスの送信元クライアントを突き止め、この不正アクセスをおこなったクライアントのIPアドレスなどの送信元情報をファイアウォール用のコンピュータ内に蓄積することにより、この送信元情報を含んだクライアントからのアクセス要求を不正アクセスとして拒絶することがファイアウォールにおいて一般的におこなわれている。

【0008】

【発明が解決しようとする課題】

しかしながら、上記の従来技術は、過去に不正アクセスをおこなったクライアントを不正クライアントと認定し、この不正クライアントからのアクセス要求を

不正アクセスとして拒絶するものであるため、不正クライアントと認定された後の不正アクセスに対してはサーバを防御することができるが、不正クライアントと認定されていないクライアントからの不正アクセスに対してはサーバを防御することができないという問題点があった。すなわち、不正クライアントと認定される前の初回の不正アクセスに対してはサーバを防御することができない。

【 0 0 0 9 】

このため、不正クライアントと認定されていないクライアントからの不正アクセスに対していかにサーバを防御するかが極めて重要な課題となっており、望ましくは、アクセス要求の送信元情報を考慮することなく、正当なアクセス要求であるか不正なアクセス要求であるか否かを判定する枠組みが必要とされている。

【 0 0 1 0 】

そこで、この発明は、上述した従来技術による問題点を解消するためになされたものであり、不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができるフィルタリング装置、フィルタリング方法およびこの方法をコンピュータに実行させるプログラムを提供することを目的とする。

【 0 0 1 1 】

【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、請求項 1、8 または 9 の発明によれば、図 1 に示す見積部 3 2 は、Web サーバ 4 0 に対する不正アクセスのパターンを格納した不正リクエスト DB（データベース）3 3 を参照し、不正アクセスのパターンおよび所定の見積ルール 3 2 a に基づいてクライアント装置 1 0 からのアクセス要求の正当性を見積もり、判定部 3 4 は、見積部 3 2 による見積結果および所定の判定ルール 3 4 a に基づいてアクセス要求を Web サーバ 4 0 に受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみを Web サーバ 4 0 に受け渡すことができ、もって不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対しても Web サーバ 4 0 を防御することができ

る。

【 0 0 1 2 】

また、請求項 2 の発明によれば、図 1 に示す見積部 3 2 は、クライアント装置 1 0 からのアクセス要求が不正リクエスト DB 3 3 に格納された不正アクセスの 패턴のいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、クライアント装置 1 0 からのアクセス要求が不正リクエスト DB 3 3 に格納された不正アクセスの 패턴のいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、判定部 3 4 は、見積部 3 2 により不正アクセスである旨が見積もられたアクセス要求を Web サーバ 4 0 に受け渡さないものと判定するとともに、見積部 3 2 により正当アクセスである旨が見積もられたアクセス要求を Web サーバ 4 0 に受け渡すものと判定することとしたので、アクセス要求が不正リクエストの 패턴に一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対しても迅速かつ確実に Web サーバ 4 0 を防御することができる。

【 0 0 1 3 】

また、請求項 3 の発明によれば、図 1 に示す見積部 3 2 は、クライアント装置 1 0 からのアクセス要求が不正リクエスト DB 3 3 に格納された不正アクセスの 패턴に該当する度合に応じて所定の見積値を算出し、判定部 3 4 は、見積部 3 2 により算出された見積値と所定の閾値とを比較してアクセス要求を Web サーバ 4 0 に受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対してもある程度の幅を持って Web サーバ 4 0 を防御することができる。

【 0 0 1 4 】

また、請求項 4 の発明によれば、図 5 に示す事前判定部 7 1 は、見積部 3 2 による正当性を見積もりの前に、Web サーバ 4 0 に対する正当アクセスの 패턴を格納した正当リクエスト DB 7 2 を参照し、クライアント装置 1 0 からのア

クセス要求が正当リクエストDB 7 2に格納された正当アクセスのパターンのいずれかに該当するか否かを判定し、見積部 3 2は、事前判定部 7 1により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくWebサーバ4 0に受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【 0 0 1 5 】

また、請求項 5の発明によれば、図 1に示す外部通報部 3 7は、所定の通報ルール 3 7 aに基づいて、判定部 3 4によりWebサーバ4 0に受け渡さないものと判定されたアクセス要求を所定の外部装置 5 0に送信することとしたので、不正アクセスに関する情報をWebサーバ4 0の管理者、リクエストフィルタ 3 0の管理者、サーバ装置 2 0全体の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に通報することができ、もってかかる管理者に対しWebサーバ4 0の保全対策を迅速に促すことができる。

【 0 0 1 6 】

また、請求項 6の発明によれば、図 1に示すログ管理部 3 6は、所定の管理ルール 3 6 aに基づいて、判定部 3 4によりWebサーバ4 0に受け渡さないものと判定されたアクセス要求を所定の格納媒体 3 6 bに格納することとしたので、格納媒体 3 6 bに格納された不正アクセスに関する情報を分析することなどができ、もってWebサーバ4 0の更なる保全対策を講じることができる。

【 0 0 1 7 】

また、請求項 7の発明によれば、図 1に示す更新部 3 9は、所定の更新ルール 3 9 aに基づいて、不正リクエストDB 3 3、正当リクエストDB 7 2（図 5に示す）、見積ルール 3 2 a、判定ルール 3 4 a、通報ルール 3 7 a、管理ルール 3 6 aまたは更新ルール 3 9 aを更新することとしたので、新たに発見された不正アクセスのパターンを不正リクエストDB 3 3に登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【 0 0 1 8 】

【発明の実施の形態】

以下に添付図面を参照して、この発明に係るフィルタリング装置、フィルタリング方法、およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。なお、以下に示す実施の形態 1 ～ 3 では、本発明に係るフィルタリング技術を、クライアント装置からの HTTP (HyperText Transfer protocol) リクエストに応じてサービスを提供するサーバ装置に適用した場合について説明する。

【 0 0 1 9 】

(実施の形態 1)

本実施の形態 1 では、クライアント装置からの HTTP リクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明する。

【 0 0 2 0 】

(1) システムの全体構成

まず最初に、本実施の形態 1 に係るクライアントサーバシステムの構成について説明する。図 1 は、本実施の形態 1 に係るクライアントサーバシステムの構成を示すブロック図である。同図に示すように、本実施の形態 1 に係るクライアントサーバシステムは、Web ブラウザ 11 をそれぞれ有する複数のクライアント装置 10 と、フィルタリング装置としてのリクエストフィルタ 30 および Web サーバ 40 を有するサーバ装置 20 とを、インターネットなどのネットワーク 1 を介して相互に通信可能に接続して構成される。

【 0 0 2 1 】

概略的に、このクライアントサーバシステムにあつては、クライアント装置 10 は、ブラウザ 11 によりサーバ装置 20 に対して HTTP リクエストなどの各種の処理要求をおこない、サーバ装置 20 の Web サーバ 40 は、クライアント装置 10 からの HTTP リクエストに応じたサービスをクライアント装置 10 に提供する。そして、サーバ装置 20 のリクエストフィルタ 30 は、クライアント装置 10 と Web サーバ 40 との間に介在し、クライアント装置 10 からの HT

ＴＰリクエストのうちの正当なリクエストのみをＷｅｂサーバ４０に受け渡す。

【 0 0 2 2 】

ここで、本実施の形態１に係るクライアントサーバシステムは、サーバ装置２０のリクエストフィルタ３０によるフィルタリング処理に特徴があり、具体的には、リクエストフィルタ３０の見積部３２は、クライアント装置１０からのＨＴＴＰリクエストが不正リクエストＤＢ３３に格納された不正アクセスのパターンのいずれかに該当する場合には不正アクセスである旨を見積もり、判定部３４は、見積部３２により不正アクセスである旨が見積もられたＨＴＴＰリクエストをＷｅｂサーバ４０に受け渡さないものと判定することにより、ＨＴＴＰリクエストの送信元情報を問題とすることなく、正当なＨＴＴＰリクエストのみをＷｅｂサーバ４０に受け渡すことができるように構成している。

【 0 0 2 3 】

(２) クライアント装置の構成

次に、図１に示したクライアント装置１０の構成について説明する。同図に示すように、クライアント装置１０は、Ｗｅｂブラウザ１１を備え、基本的には、サーバ装置２０に対してＨＴＴＰリクエストなどの処理要求をおこない、サーバ装置２０のＷｅｂサーバ４０により提供されるＷｅｂデータを解釈して、モニタなどの出力部に表示させる表示制御（ブラウズ処理）をおこなう。

【 0 0 2 4 】

そして、このクライアント装置１０は、悪意を持った使用方法によってサーバ装置２０に対して不正アクセスをおこなうことができる装置でもある。すなわち、クライアント装置１０は、侵入者（イントルダ）や攻撃者（アタッカ）などの悪意を持ったユーザの使用によっては、Ｗｅｂサーバ４０上のパスワードファイルなどのリモートユーザが見るべきでないファイルを見たり、Ｗｅｂサーバ４０上に存在しないファイルをリクエストしてＷｅｂサーバ４０の機能を停止させたり、コマンド文字列を含んだリクエストによりＷｅｂサーバ４０上で任意のシステムコマンドを実行するなどの不正アクセスをおこない得るものである。このようなクライアント装置１０による不正アクセスに対してＷｅｂサーバ４０を防御するのがリクエストフィルタ３０の役割である。

【 0 0 2 5 】

なお、クライアント装置 1 0 は、たとえば、パーソナルコンピュータやワークステーション、家庭用ゲーム機、インターネットTV、PDA(Personal Digital Assistant)、あるいは、携帯電話やPHS(Personal Handy Phone System)の如き移動体通信端末によって実現することができる。また、クライアント装置 1 0 は、モデム、TA、ルータなどの通信装置と電話回線を介して、あるいは、専用線を介して、ネットワーク 1 に接続されており、所定の通信規約（たとえば、TCP/IPインターネットプロトコル）に従ってサーバ装置 2 0 にアクセスすることができる。

【 0 0 2 6 】

(3) サーバ装置におけるWebサーバの構成

次に、図 1 に示したサーバ装置 2 0 におけるWebサーバ 4 0 の構成について説明する。同図に示すように、サーバ装置 2 0 のWebサーバ 4 0 は、リクエストフィルタ 2 0 を介してクライアント装置 1 0 からのHTTPリクエストを受信し、このHTTPリクエストに応じてHTML(HyperText Markup Language)などのマークアップ言語により記述された各種の情報を送信するなどのサービスをクライアント装置 1 0 に提供する。

【 0 0 2 7 】

このWebサーバ 4 0 は、機能概念的には、一般的なWebサーバと同様の動作をおこなうものであるが、ここでのWebサーバ 4 0 は、一般的なWebサーバと異なり、サーバ装置 2 0 においてHTTPリクエストに割り当てられるポート番号 8 0 のTCP(Transmission Control Protocol)ポートを監視することはおこなわない。

【 0 0 2 8 】

すなわち、クライアント装置 1 0 からのHTTPリクエストをWebサーバ 4 0 により直接に受信するのではなく、リクエストフィルタ 3 0 がHTTPリクエストを受信し、プロセス間通信をおこなって正当なHTTPリクエストのみをWebサーバ 4 0 に受け渡すこととしている。

【 0 0 2 9 】

(4) サーバ装置におけるリクエストフィルタの構成

次に、図 1 に示したサーバ装置 2 0 におけるリクエストフィルタ 3 0 の構成について説明する。同図に示すように、リクエストフィルタ 3 0 は、受信部 3 1 と、見積部 3 2 と、不正リクエスト DB 3 3 と、判定部 3 4 と、送信部 3 5 と、ログ管理部 3 6 と、外部通報部 3 7 と、外部情報取得部 3 8 と、更新部 3 9 とを備える。

【 0 0 3 0 】

このうち、受信部 3 1 は、サーバ装置 2 0 におけるポート番号 8 0 の T C P ポートを監視して、クライアント装置 1 0 からの H T T P リクエストを W e b サーバ 4 0 が受信する前に受信する処理部である。なお、受信部 3 1 によりクライアント装置 1 0 から受信した H T T P リクエストは、見積部 3 2 および送信部 3 3 に出力される。

【 0 0 3 1 】

見積部 3 2 は、不正リクエスト DB 3 3 に格納された不正アクセスのパターンおよび所定の見積ルール 3 2 a に基づいて H T T P リクエストの正当性を見積もり、その見積結果を判定部 3 4 に出力する処理部である。

【 0 0 3 2 】

ここで、見積部 3 2 が見積もりに際して参照する不正リクエスト DB 3 3 について説明する。図 2 は、不正リクエスト DB 3 3 に格納される情報の構成例を示す図である。同図に示すように、不正リクエスト DB 3 3 は、サーバに対する不正アクセスのパターンを格納したデータベースであり、ネットワーク世界で収集された不正アクセスを図示のような形式言語を用いて記述した複数のパターンを記憶している。

【 0 0 3 3 】

例えば、同図に示す「URL=</>」のパターンは、URL (Uniform Resource Locator) の先頭が「/」である不正リクエストを意味し、「CGI==p h f、ARG=<Q n a m e=r o o t % O A」のパターンは、CGI (Common Gateway Interface) 名が「p h f」であり、そのある引数の先頭が「Q n a m e=r o o t % O A」である不正リクエストを意味し、「URL<>」.

¥. . ¥. . ¥. . 」のパターンは、URLに「. . ¥. . ¥. . ¥. . 」が含まれる不正リクエストを意味し、「CGI>=. h t r」のパターンは、CGI名の末尾が「. h t r」である不正リクエストを意味する。

【 0 0 3 4 】

なお、図2には示していないが、不正リクエストDB33には、Webサーバ40上で任意のシステムコマンドを実行するような不正なコマンド文字列も複数記憶されている。このようなコマンド文字列のパターンを記憶することにより、攻撃方法が既知である不正アクセスだけでなく、攻撃方法が未知である不正アクセスに対してもWebサーバ40を防御することができる。

【 0 0 3 5 】

このような不正リクエストDB33を参照することにより、見積部32は、所定の見積ルール32aに基づいてHTTPリクエストの正当性を見積もりをおこなう。具体的には、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンのいずれかに該当する場合には、該HTTPリクエストは不正アクセスである旨を見積もり、一方、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンのいずれにも該当しない場合には、該HTTPリクエストは正当アクセスである旨を見積もる。

【 0 0 3 6 】

図1の説明に戻ると、判定部34は、見積部32から受け取った見積結果および所定の判定ルール34aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否かを判定し、この判定結果を送信部35に出力する処理部である。具体的には、見積部32から不正アクセスである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡さないものと判定し（不可判定）、一方、見積部32から正当アクセスである旨の見積結果を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡すものと判定する（可判定）。

【 0 0 3 7 】

送信部35は、判定部34から受け取った判定結果に基づいて、受信部31から受け取ったHTTPリクエストの送信を制御する処理部である。具体的には、

判定部 3 4 から可判定を受け取った場合には、H T T P リクエストをプロセス間通信により W e b サーバ 4 0 に受け渡す。一方、判定部 3 4 から不可判定を受け取った場合には、H T T P リクエストの W e b サーバ 4 0 への受け渡しを拒絶して、この不正リクエストを破棄する。

【 0 0 3 8 】

ログ管理部 3 6 は、所定の管理ルール 3 6 a に基づいて、判定部 3 4 により W e b サーバ 4 0 に受け渡さないものと判定された不正リクエストに係る情報を格納媒体 3 6 b に格納して管理する処理部である。具体的には、管理ルール 3 6 a に基づいて、不正リクエストの内容、送信元情報（I P アドレスやホスト名）、送信時刻、見積部 3 2 による見積結果の根拠、判定部 3 4 による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に格納媒体 3 6 b に格納する。例えば、攻撃性の高い不正リクエストのみを格納するなどである。

【 0 0 3 9 】

なお、格納媒体 3 6 b に格納された情報は、該格納媒体 3 6 b を取り出すことや通信回線を介することなどによりサーバ装置 2 0 の外部に出力することができ、さらに、格納媒体 3 6 b に格納された情報を分析して不正アクセスの傾向などを解析することにより、W e b サーバ 4 0 の更なる保全のために対策を講じることがもできる。

【 0 0 4 0 】

外部通報部 3 7 は、所定の通報ルール 3 7 a に基づいて、判定部 3 4 により W e b サーバ 4 0 に受け渡さないものと判定された不正リクエストに係る情報を外部装置 5 0 に通報する処理部である。具体的には、ログ管理部 3 6 による処理と同様、通報ルール 3 7 a に基づいて、不正リクエストの内容、送信元情報（I P アドレスやホスト名）、送信時刻、見積部 3 2 による見積結果の根拠、判定部 3 4 による判定結果の根拠などの不正リクエストに係る情報を選択的に編集するとともに、この選択編集された情報を不正リクエストの攻撃性の高低などに応じて選択的に外部装置 5 0 に通報する。

【 0 0 4 1 】

この外部通報部 3 8 から通報を受ける外部装置 5 0 は、W e b サーバ 4 0 の管理者、リクエストフィルタ 3 0 の管理者、サーバ装置 2 0 全体の管理者、ネットワーク全般を監視する公的な機関（管理センタ）の管理者など（以下、これらを総称して「管理者」という。）が操作する通信装置である。そして、外部通報部 3 7 は、例えば、攻撃性の高い不正リクエストについてはリアルタイムで迅速に管理者に通報し、攻撃性の低い不正リクエストについては非リアルタイムで一括して管理者に通報するなどして、かかる通報を受ける管理者に対して W e b サーバ 4 0 の保全対策を迅速に促すことができる。

【 0 0 4 2 】

外部情報取得部 3 8 は、所定の取得ルール 3 8 a に基づいて、更新部 3 9 による更新処理に用いられる情報を、外部装置 5 0 や W e b サーバ 4 0 などのリクエストフィルタ 3 0 の外部から能動的または受動的に取得する処理部である。例えば、管理者が外部装置 5 0 を介して入力した新たな不正リクエストのパターンや、管理者が外部装置 5 0 を介して入力した見積ルール 3 2 a の変更指示情報などを取得するほか、不正リクエストによる被害を受けた W e b サーバ 4 0 から被害の状況や不正アクセスの内容などの情報を取得する。なお、所定の取得ルール 3 8 a は、権限が認証された管理者からの情報のみを取得するなどの規則である。

【 0 0 4 3 】

更新部 3 9 は、所定の更新ルール 3 9 a に基づいて、不正リクエスト D B 3 3 、見積ルール 3 2 a 、判定ルール 3 4 a 、管理ルール 3 6 a 、通報ルール 3 7 a 、取得ルール 3 8 a または更新ルールに格納された情報を更新する処理部である。例えば、外部情報取得部 3 8 から新たな不正リクエストのパターンを受け付けた場合には、この不正リクエストのパターンを不正リクエスト D B 3 3 に格納し、また見積ルール 3 2 a の変更指示情報を受け付けた場合には、この変更指示情報に応じて見積ルール 3 2 a を変更する。このような更新処理をおこなうことにより、日々進化する不正アクセスに対して機動的に対応することができる。

【 0 0 4 4 】

（ 5 ） フィルタリング処理

次に、本実施の形態 1 によるフィルタリングの処理手順について説明する。図

3は、本実施の形態1によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置20におけるリクエストフィルタ30の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する（ステップS301）。

【0045】

そして、リクエストフィルタ30の見積部32は、不正リクエストDB33に格納された不正アクセスのパターンおよび所定の見積ルール32aに基づいてHTTPリクエストの正当性を見積もる（ステップS302）。具体的には、HTTPリクエストが不正アクセスのパターンのいずれかに該当する場合には、不正リクエストである旨を見積もり、一方、HTTPリクエストが不正アクセスのパターンのいずれにも該当しない場合には、正当リクエストである旨を見積もる。

【0046】

その後、リクエストフィルタ30の判定部34は、見積部32から受け取った見積結果および所定の判定ルール34aに基づいてHTTPリクエストをWebサーバ40に受け渡すか否かを判定する（ステップS303）。具体的には、見積部32により正当なリクエストである旨が見積もられたか否かを判定する。

【0047】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップS303肯定）、リクエストフィルタ30の送信部35は、HTTPリクエストをプロセス間通信によりWebサーバ40に受け渡し（ステップS304）、Webサーバ40は、HTTPリクエストに応じた情報をクライアント装置10に送信するなどの正当判定時の処理をおこなう（ステップS305）。

【0048】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップS303否定）、リクエストフィルタ30の送信部35は、HTTPリクエストのWebサーバ40への受け渡しを拒絶し（ステップS306）、リクエストフィルタ30の各部は、不正リクエストの破棄、格納媒体36bへの格納、外部装置50への通報などの不正判定時の処理をおこなう（ステッ

プ S 3 0 7)。

【 0 0 4 9 】

上述してきたように、本実施の形態 1 によれば、アクセス要求の送信元情報ではなく、アクセス要求の具体的な要求内容が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができる。これにより、不正クライアントと認定されていないクライアント装置 1 0 からの不正アクセスに対しても迅速かつ確実に W e b サーバ 4 0 を防御することができる。

【 0 0 5 0 】

(実施の形態 2)

ところで、上記実施の形態 1 では、クライアント装置からの H T T P リクエストが不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを判定する場合について説明したが、本発明はこれに限定されるものではなく、H T T P リクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合についても同様に適用することができる。

【 0 0 5 1 】

そこで、本実施の形態 2 では、H T T P リクエストが不正アクセスのパターンに該当する度合に応じて不正アクセスであるか否かを判定する場合について説明する。なお、本実施の形態 2 においては、クライアントサーバシステムのシステム構成は図 1 に示すものと同様のものとなるので、ここではその詳細な説明を省略する。

【 0 0 5 2 】

まず最初に、本実施の形態 2 の特徴部分である見積部 3 2 および判定部 3 4 について説明する。本実施の形態 2 における見積部 3 2 は、クライアント装置 1 0 からの H T T P リクエストが不正リクエスト D B 3 3 に格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、その見積値を判定部 3 4 に出力する。

【 0 0 5 3 】

具体的には、不正アクセスのパターンから一致するパターンの個数を算出する

ことや、各パターンに危険度を付与して一致するパターンの危険度を算出することなどにより、HTTPリクエストの危険度を示すDI (Danger Index) と呼ばれる見積値を算出する。なお、見積値DIは、例えば1～100の範囲で整数値をとり、危険度が高いHTTPリクエストほど大きな値が算出されるというものである。

【0054】

本実施の形態2における判定部34は、見積部32により算出された見積値DIと所定の閾値とを比較してHTTPリクエストをWebサーバ40に受け渡すか否かを判定し、この判定結果を送信部35に出力する。

【0055】

具体的には、所定の閾値を50と仮定すると、見積部32からDIが50以上である見積値を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡さないものと判定し（不可判定）、一方、見積部32からDIが50未満である見積値を受け取った場合には、HTTPリクエストをWebサーバ40に受け渡すものと判定する（可判定）。

【0056】

次に、本実施の形態2によるフィルタリングの処理手順について説明する。図4は、本実施の形態2によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置20におけるリクエストフィルタ30の受信部31は、クライアント装置10からのHTTPリクエストをWebサーバ40が受信する前に受信する（ステップS401）。

【0057】

そして、リクエストフィルタ30の見積部32は、HTTPリクエストが不正リクエストDB33に格納された不正アクセスのパターンに該当する度合に応じて見積値DIを算出する（ステップS402）。リクエストフィルタ30の判定部34は、見積部32により算出された見積値DIと所定の閾値とを比較してHTTPリクエストをWebサーバ40に受け渡すか否かを判定する（ステップS403）。具体的には、見積値DIが所定の閾値以上であるか否かを判定する。

【0058】

この判定により、見積値D I が所定の閾値未満であると判定された場合には（ステップS 4 0 3 肯定）、リクエストフィルタ3 0 の送信部3 5 は、H T T P リクエストをプロセス間通信によりW e b サーバ4 0 に受け渡し（ステップS 4 0 4）、W e b サーバ4 0 は、H T T P リクエストに応じた情報をクライアント装置1 0 に送信するなどの正当判定時の処理をおこなう（ステップS 4 0 5）。

【0 0 5 9】

これとは反対に、見積値D I が所定の閾値以上であると判定された場合には（ステップS 4 0 3 否定）、リクエストフィルタ3 0 の送信部3 5 は、H T T P リクエストのW e b サーバ4 0 への受け渡しを拒絶し（ステップS 4 0 6）、リクエストフィルタ3 0 の各部は、不正リクエストの破棄、格納媒体3 6 b への格納、外部装置5 0 への通報などの不正判定時の処理をおこなう（ステップS 4 0 7）。

【0 0 6 0】

上述してきたように、本実施の形態2 によれば、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができる。これにより、不正クライアントと認定されていないクライアント装置1 0 からの不正アクセスに対してもある程度の幅を持ってW e b サーバ4 0 を防御することができる。

【0 0 6 1】

（実施の形態3）

ところで、上記実施の形態1 および2 では、クライアント装置からの全てのH T T P リクエストについて不正アクセスのパターンに基づく見積もりをおこなう場合について説明したが、本発明にはこれに限定されるものではなく、一部のH T T P リクエストについてのみ見積もりをおこなう場合についても同様に適用することができる。

【0 0 6 2】

そこで、本実施の形態3 では、二階層からなるフィルタリング処理をおこない、一部のH T T P リクエストについてのみ不正アクセスのパターンに基づく見積もりをおこなう場合について説明する。

【 0 0 6 3 】

図 5 は、本実施の形態 3 に係るクライアントサーバシステムの構成を示すブロック図である。なお、図 1 に示した各部と同様の機能を有する部位には同一符号を付すこととしてその詳細な説明を省略し、本実施の形態 3 の特徴部分である事前判定部 7 1 および正当リクエスト DB 7 2 について説明する。

【 0 0 6 4 】

サーバ装置 6 0 におけるリクエストフィルタ 7 0 の事前判定部 7 1 は、見積部 3 2 による正当性を見積もりの前に、正当リクエスト DB 7 2 に格納された正当アクセスのパターンおよび所定の事前判定ルール 7 1 a に基づいて HTTP リクエストの見積もりを省くことができるか否かを判定する処理部である。

【 0 0 6 5 】

ここで、事前判定部 7 1 が判定に際して参照する正当リクエスト DB 7 2 について説明すると、この正当リクエスト DB 7 2 は、Web サーバ 4 0 に対する正当アクセスのパターンを格納したデータベースであり、具体的には、Web サーバ 4 0 上に存在するファイルのうちでリモートユーザに見られても構わないファイルのパスを記憶する。

【 0 0 6 6 】

このリモートユーザに見られても構わないファイルとは、パスワードファイルなどのリモートユーザが見るべきでないファイル以外のファイルであって、例えば、Web サーバ 4 0 に対する HTTP リクエストのリクエスト内容として非常に高い割合を有する画像ファイルなど、不正アクセスの可能性がほとんどないようなファイルが含まれる。

【 0 0 6 7 】

このような正当リクエスト DB 7 2 を参照することにより、事前判定部 7 1 は、所定の事前判定ルール 7 1 a に基づいて HTTP リクエストの見積もりを省くことができるか否かを判定する。具体的には、HTTP リクエストが正当リクエスト DB 7 2 に格納された正当アクセスのパターンのいずれかに該当する場合には、該 HTTP リクエストの見積もりを省くことができるものと判定し、一方、HTTP リクエストが正当リクエスト DB 7 2 に格納された正当アクセスのパタ

ーンのいずれにも該当しない場合には、該HTTPリクエストの見積もりを省くことができないものと判定する。

【 0 0 6 8 】

そして、事前判定部 7 1 は、見積もりを省くことができないものと判定された HTTP リクエストのみを見積部 3 2 に出力し、見積もりを省くことができるものと判定された HTTP リクエストについては、見積部 3 2 および判定部 3 4 による処理を省いて、送信部 3 5 を介して Web サーバ 4 0 に受け渡す。

【 0 0 6 9 】

なお、正当リクエスト DB 7 2 に格納される正当アクセスのパターンは、Web サーバ 4 0 に新たな画像ファイルが追加された場合などに応じて、更新部 3 9 により更新される。

【 0 0 7 0 】

次に、本実施の形態 3 によるフィルタリングの処理手順について説明する。図 6 は、本実施の形態 3 によるフィルタリングの処理手順を説明するフローチャートである。同図に示すように、サーバ装置 6 0 におけるリクエストフィルタ 7 0 の受信部 3 1 は、クライアント装置 1 0 からの HTTP リクエストを Web サーバ 4 0 が受信する前に受信する（ステップ S 6 0 1）。

【 0 0 7 1 】

そして、リクエストフィルタ 7 0 の事前判定部 7 1 は、正当リクエスト DB 7 2 に格納された正当アクセスのパターンおよび所定の事前判定ルール 7 1 a に基づいて HTTP リクエストの見積もりを省くことができるか否かを判定する（ステップ S 6 0 2）。具体的には、HTTP リクエストが正当リクエスト DB 7 2 に格納された正当アクセスのパターンのいずれかに該当するか否かを判定する。

【 0 0 7 2 】

この判定により、正当アクセスのパターンのいずれかに該当するものと判定された場合には（ステップ S 6 0 2 肯定）、この HTTP リクエストの正当性を見積もりを省き、リクエストフィルタ 7 0 の送信部 3 5 は、HTTP リクエストをプロセス間通信により Web サーバ 4 0 に受け渡し（ステップ S 6 0 5）、Web サーバ 4 0 は、HTTP リクエストに応じた情報をクライアント装置 1 0 に送

信するなどの正当判定時の処理をおこなう（ステップ S 6 0 6）。

【 0 0 7 3 】

これとは反対に、正当アクセスのパターンのいずれにも該当しないものと判定された場合には（ステップ S 6 0 2 否定）、この HTTP リクエストを見積部 3 2 に受け渡し、上記実施の形態 1 または 2 によるフィルタリング処理と同様の処理をおこなう（ステップ S 6 0 3 ～ 6 0 8）。

【 0 0 7 4 】

すなわち、リクエストフィルタ 7 0 の見積部 3 2 は、HTTP リクエストの正当性を見積もり（ステップ S 6 0 3）、判定部 3 4 は、HTTP リクエストを Web サーバ 4 0 に受け渡すか否かを判定する（ステップ S 6 0 4）。

【 0 0 7 5 】

この判定により、正当なリクエストである旨が見積もられたものと判定された場合には（ステップ S 6 0 4 肯定）、リクエストフィルタ 7 0 の送信部 3 5 は、HTTP リクエストをプロセス間通信により Web サーバ 4 0 に受け渡し（ステップ S 6 0 5）、Web サーバ 4 0 は、HTTP リクエストに応じた情報をクライアント装置 1 0 に送信するなどの正当判定時の処理をおこなう（ステップ S 6 0 6）。

【 0 0 7 6 】

これとは反対に、不正なリクエストである旨が見積もられたものと判定された場合には（ステップ S 6 0 4 否定）、リクエストフィルタ 7 0 の送信部 3 5 は、HTTP リクエストの Web サーバ 4 0 への受け渡しを拒絶し（ステップ S 6 0 7）、リクエストフィルタ 7 0 の各部は、不正リクエストの破棄、格納媒体 3 6 b への格納、外部装置 5 0 への通報などの不正判定時の処理をおこなう（ステップ S 6 0 8）。

【 0 0 7 7 】

上述してきたように、本実施の形態 3 によれば、画像ファイルを要求する HTTP リクエストのような要求の割合は高いが攻撃性は極めて低いものについては、見積部 3 2 および判定部 3 3 による処理を省いて迅速な処理をおこなうことができるとともに、パスワードファイルや Web サーバ 4 0 上に存在しないファイ

ルを要求するHTTPリクエストのような攻撃性が高いものについては、見積部32および判定部33による処理をおこなって、かかる攻撃を有効に防御することができる。

【0078】

なお、本実施の形態1～3では、クライアント装置10からのHTTPリクエストをフィルタリングする場合について説明したが、本発明はこれに限定されるものではなく、FTP (File Transfer Protocol)、telnet、コンソールなど、クライアント装置10からWebサーバ40に入力されるあらゆる情報をフィルタリングする場合に同様に適用することができる。

【0079】

また、本実施の形態1～3では、フィルタリング装置としてのリクエストフィルタ30、70をサーバ装置40、60に設けた場合について説明したが、本発明はこれに限定されるものではなく、例えば、それぞれのクライアント装置側にリクエストフィルタを設けたり、一つのリクエストフィルタにより複数のWebサーバを防御するなど、クライアント装置とWebサーバとの間にリクエストフィルタが介在するあらゆるシステム構成において同様に適用することができる。

【0080】

なお、本実施の形態1～3で説明したフィルタリング方法は、あらかじめ用意されたプログラムをパーソナル・コンピュータやワークステーションなどのコンピュータで実行することによって実現することができる。このプログラムは、インターネットなどのネットワークを介して配布することができる。また、このプログラムは、ハードディスク、フロッピーディスク、CD-ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行することもできる。

【0081】

(付記1) クライアントと該クライアントからのアクセス要求に応じてサービスを提供するサーバとの間に介在し、前記アクセス要求のうちの正当なアクセス要求のみを前記サーバに受け渡すフィルタリング装置において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベ

ースと、

前記不正パターンデータベースに格納された不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積手段と、

前記見積手段による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定手段と、

を備えたことを特徴とするフィルタリング装置。

【 0 0 8 2 】

（付記 2）前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定手段は、前記見積手段により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積手段により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 1 に記載のフィルタリング装置。

【 0 0 8 3 】

（付記 3）前記見積手段は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定手段は、前記見積手段により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記 1 に記載のフィルタリング装置。

【 0 0 8 4 】

（付記 4）前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースと、前記見積手段による正当性を見積もりの前に、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定手段と、をさらに備え、前記見積手段は、前記事前判定手段により正当アクセスのパターンに該当しないものと判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 1、2 ま

たは 3 に記載のフィルタリング装置。

【 0 0 8 5 】

（付記 5）所定の外部送信ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信手段をさらに備えたことを特徴とする付記 1 ～ 4 のいずれか一つに記載のフィルタリング装置。

【 0 0 8 6 】

（付記 6）所定の格納ルールに基づいて、前記判定手段により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納手段をさらに備えたことを特徴とする付記 1 ～ 5 のいずれか一つに記載のフィルタリング装置。

【 0 0 8 7 】

（付記 7）所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新手段をさらに備えたことを特徴とする付記 1 ～ 6 のいずれか一つに記載のフィルタリング装置。

【 0 0 8 8 】

（付記 8）クライアントからのアクセス要求に応じてサービスを提供するサーバに対し、前記クライアントからのアクセス要求のうちの正当なアクセス要求のみを受け渡すフィルタリング方法において、

前記サーバに対する不正アクセスのパターンを格納した不正パターンデータベースを参照し、該参照した不正アクセスのパターンおよび所定の見積ルールに基づいて前記アクセス要求の正当性を見積もる見積工程と、

前記見積工程による見積結果および所定の判定ルールに基づいて前記アクセス要求を前記サーバに受け渡すか否かを判定する判定工程と、

を含んだことを特徴とするフィルタリング方法。

【 0 0 8 9 】

（付記 9）前記見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要

求は不正アクセスである旨を見積もるとともに、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、前記判定工程は、前記見積工程により不正アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡さないものと判定するとともに、前記見積工程により正当アクセスである旨が見積もられたアクセス要求を前記サーバに受け渡すものと判定することを特徴とする付記 8 に記載のフィルタリング方法。

【 0 0 9 0 】

（付記 1 0）前記見積工程は、前記アクセス要求が前記不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、前記判定工程は、前記見積工程により算出された見積値と所定の閾値とを比較して前記アクセス要求を前記サーバに受け渡すか否かを判定することを特徴とする付記 8 に記載のフィルタリング方法。

【 0 0 9 1 】

（付記 1 1）前記見積工程による正当性を見積もりの前に、前記サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、前記アクセス要求が前記正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定する事前判定工程をさらに含み、前記見積工程は、前記事前判定工程により正当アクセスのパターンに該当しないもの判定されたアクセス要求のみについて正当性を見積もることを特徴とする付記 8、9 または 1 0 に記載のフィルタリング方法。

【 0 0 9 2 】

（付記 1 2）所定の外部送信ルールに基づいて、前記判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信する外部送信工程をさらに含んだことを特徴とする付記 8 ～ 1 1 のいずれか一つに記載のフィルタリング方法。

【 0 0 9 3 】

（付記 1 3）所定の格納ルールに基づいて、前記判定工程により前記サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納する格納工程

をさらに含んだことを特徴とする付記 8 ～ 1 2 のいずれか一つに記載のフィルタリング方法。

【 0 0 9 4 】

(付記 1 4) 所定の更新ルールに基づいて、前記不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新する更新工程をさらに含んだことを特徴とする付記 8 ～ 1 3 のいずれか一つに記載のフィルタリング方法。

【 0 0 9 5 】

(付記 1 5) 前記付記 8 ～ 1 4 のいずれか一つに記載された方法をコンピュータに実行させるプログラム。

【 0 0 9 6 】

【発明の効果】

以上説明したように、請求項 1、8 または 9 の発明によれば、サーバに対する不正アクセスのパターンを格納した不正パターンデータベースの不正アクセスのパターンおよび所定の見積ルールに基づいてアクセス要求の正当性を見積もり、この見積結果および所定の判定ルールに基づいてアクセス要求をサーバに受け渡すか否かを判定することとしたので、アクセス要求の送信元情報ではなくアクセス要求の具体的な要求内容に基づいて不正アクセスであるか否かを判定することができる。これにより、正当なアクセス要求のみをサーバに受け渡すことができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御することができる。

【 0 0 9 7 】

また、請求項 2 の発明によれば、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンのいずれかに該当する場合に該アクセス要求は不正アクセスである旨を見積もるとともに、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンのいずれにも該当しない場合に該アクセス要求は正当アクセスである旨を見積もり、不正アクセスである旨が見積もられたアクセス要求をサーバに受け渡さないものと判定するとともに、正当アクセスである旨が見積もられたアクセス要求をサーバに受け渡すものと判定する

こととしたので、アクセス要求が不正リクエストのパターンに一致するか否かによって不正アクセスであるか否かを迅速かつ確実に判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対しても迅速かつ確実にサーバを防御することができる。

【 0 0 9 8 】

また、請求項 3 の発明によれば、アクセス要求が不正パターンデータベースに格納された不正アクセスのパターンに該当する度合に応じて所定の見積値を算出し、この算出された見積値と所定の閾値とを比較してアクセス要求をサーバに受け渡すか否かを判定することとしたので、見積値および閾値の比較によってある程度の幅を持たせて不正アクセスであるか否かを判定することができ、もって不正クライアントと認定されていないクライアントからの不正アクセスに対してもある程度の幅を持ってサーバを防御することができる。

【 0 0 9 9 】

また、請求項 4 の発明によれば、正当性を見積もりの前に、サーバに対する正当アクセスのパターンを格納した正当パターンデータベースを参照し、アクセス要求が正当パターンデータベースに格納された正当アクセスのパターンのいずれかに該当するか否かを判定し、正当アクセスのパターンに該当しないもの判定されたアクセス要求のみについて正当性を見積もることとしたので、正当アクセスのパターンと一致するアクセス要求については正当性を見積もることなくサーバに受け渡す一方、正当アクセスのパターンと一致しないアクセス要求のみについて正当性を見積もることができ、もって不正アクセスであるか否かを全体としてより迅速に判定することができる。

【 0 1 0 0 】

また、請求項 5 の発明によれば、所定の外部送信ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の外部装置に送信することとしたので、不正アクセスに関する情報をサーバの管理者、フィルタリング装置の管理者、ネットワーク全般を監視する公的な機関の管理者などに迅速に送信することができ、もってかかる管理者に対しサーバの保全対策を迅速に促すことができる。

【 0 1 0 1 】

また、請求項 6 の発明によれば、所定の格納ルールに基づいて、サーバに受け渡さないものと判定されたアクセス要求を所定の格納媒体に格納することとしたので、格納媒体に格納された不正アクセスに関する情報を分析することなどができ、もってサーバの更なる保全対策を講じることができる。

【 0 1 0 2 】

また、請求項 7 の発明によれば、所定の更新ルールに基づいて、不正パターンデータベース、正当パターンデータベース、見積ルール、判定ルール、外部送信ルール、格納ルールまたは更新ルールを更新することとしたので、新たに発見された不正アクセスのパターンを不正パターンデータベースに登録することなどができ、もって日々進化する不正アクセスに対して機動的に対応することができる。

【図面の簡単な説明】

【図 1】

本実施の形態 1 に係るクライアントサーバシステムの構成を示すブロック図である。

【図 2】

不正リクエスト DB に格納される情報の構成例を示す図である。

【図 3】

本実施の形態 1 によるフィルタリングの処理手順を説明するフローチャートである。

【図 4】

本実施の形態 2 によるフィルタリングの処理手順を説明するフローチャートである。

【図 5】

本実施の形態 3 に係るクライアントサーバシステムの構成を示すブロック図である。

【図 6】

本実施の形態 3 によるフィルタリングの処理手順を説明するフローチャートで

ある。

【符号の説明】

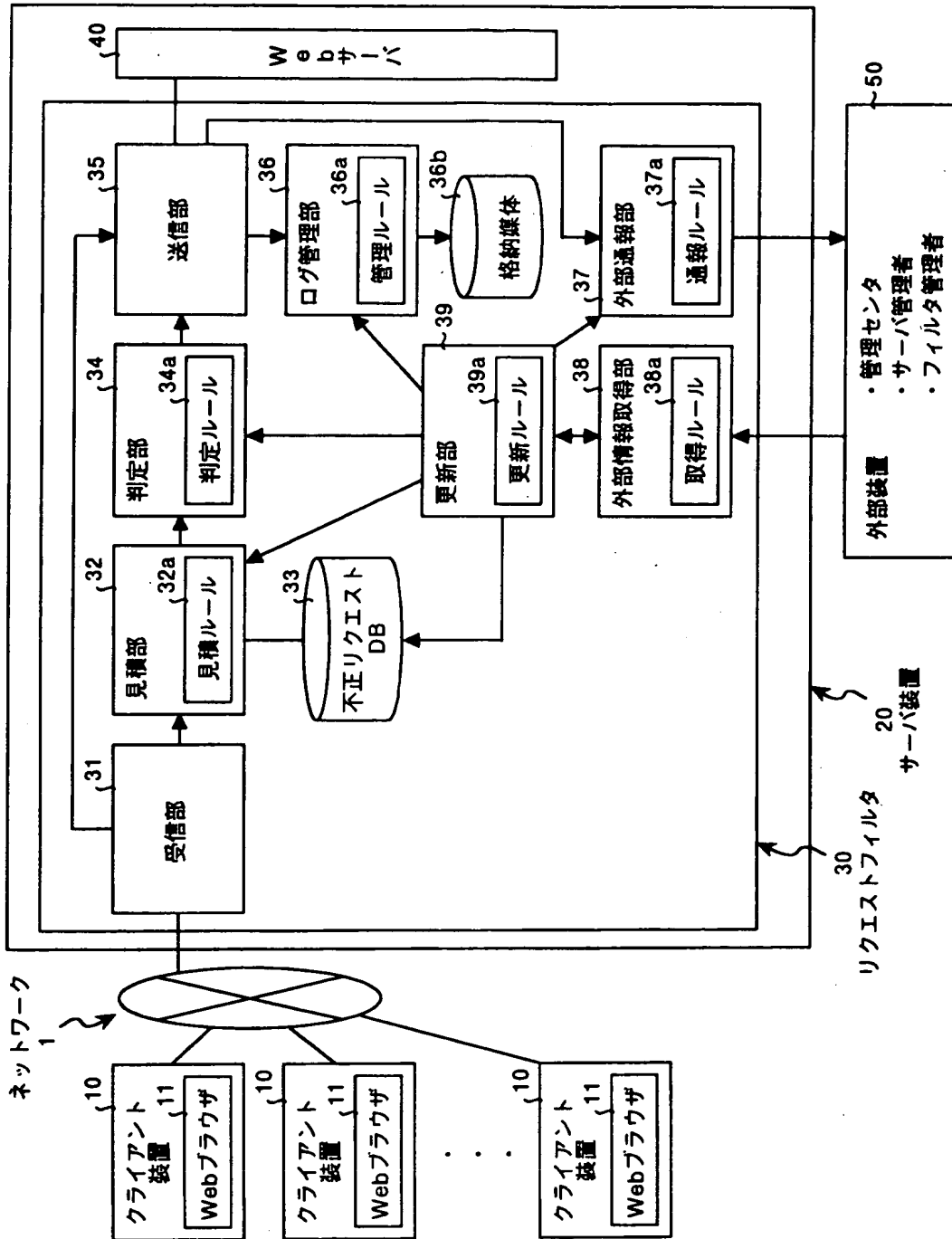
- 1 ネットワーク
- 1 0 クライアント装置
- 1 1 W e b ブラウザ
- 2 0、6 0 サーバ装置
- 3 0、7 0 リクエストフィルタ
- 3 1 受信部
- 3 2 見積もり部
- 3 2 a 見積ルール
- 3 3 不正リクエスト D B
- 3 4 判定部
- 3 4 a 判定ルール
- 3 5 送信部
- 3 6 ログ管理部
- 3 6 a 管理ルール
- 3 7 外部通報部
- 3 7 a 通報ルール
- 3 8 外部情報取得部
- 3 8 a 取得ルール
- 3 9 更新部
- 3 9 a 更新ルール
- 4 0 W e b サーバ
- 5 0 外部装置
- 7 1 事前判定部
- 7 1 a 事前判定ルール
- 7 2 正当リクエスト D B

【書類名】

図面

【図 1】

本実施の形態 1 に係るサーバクライアントシステムの構成を示すブロック図



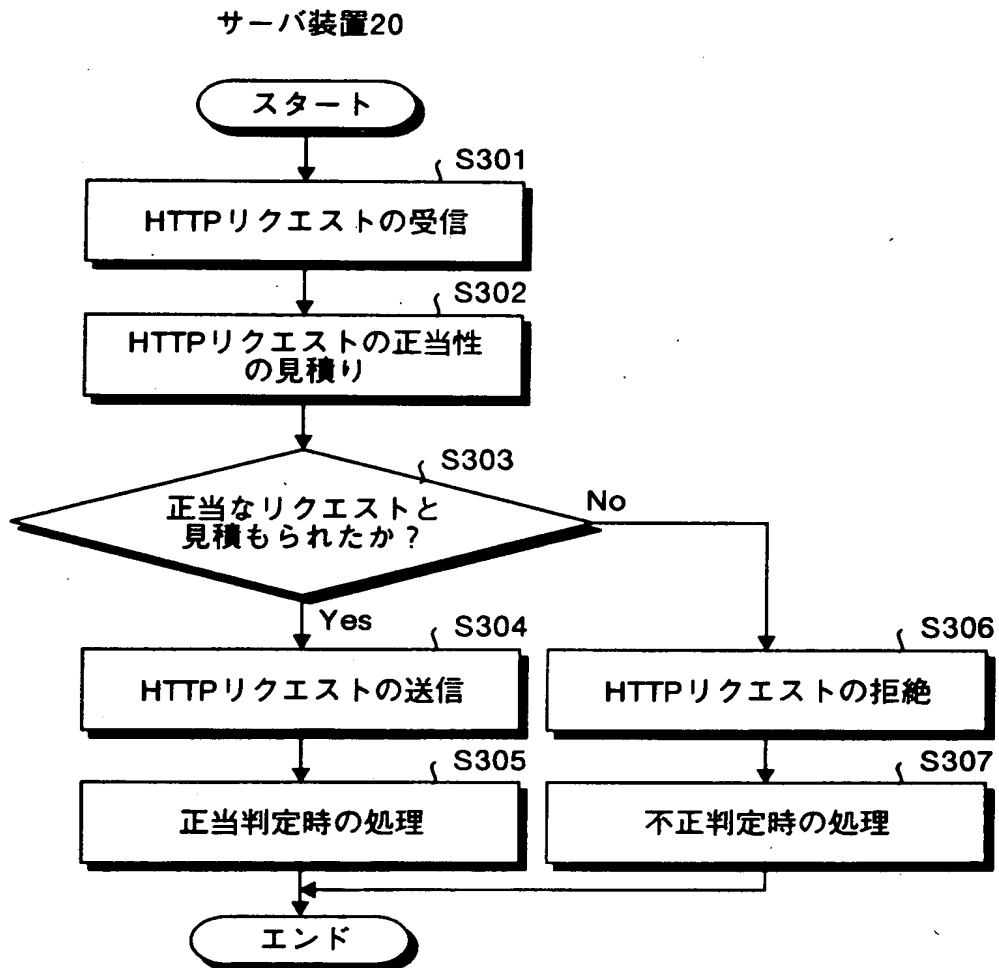
【図2】

不正リクエストDBに格納される情報の構成例を示す図

形式言語パターン	意味
URL=<//	URLの先頭が“//”と一致するリクエストを却下。
CGI==phf ARG=<Qname=root%OA	CGI名が“phf”であり、且つそのある引数の先頭が“Qname=root%OA”と一致するリクエストを却下。
URL<>..*.%.%.%	URLに“..*.%.%.%”が含まれるリクエストを却下。
CGI>=.htr	CGI名の末尾が、“htr”と一致するリクエストを却下。 すなわち、CGIが拡張子“.htr”を有するリクエストを却下。

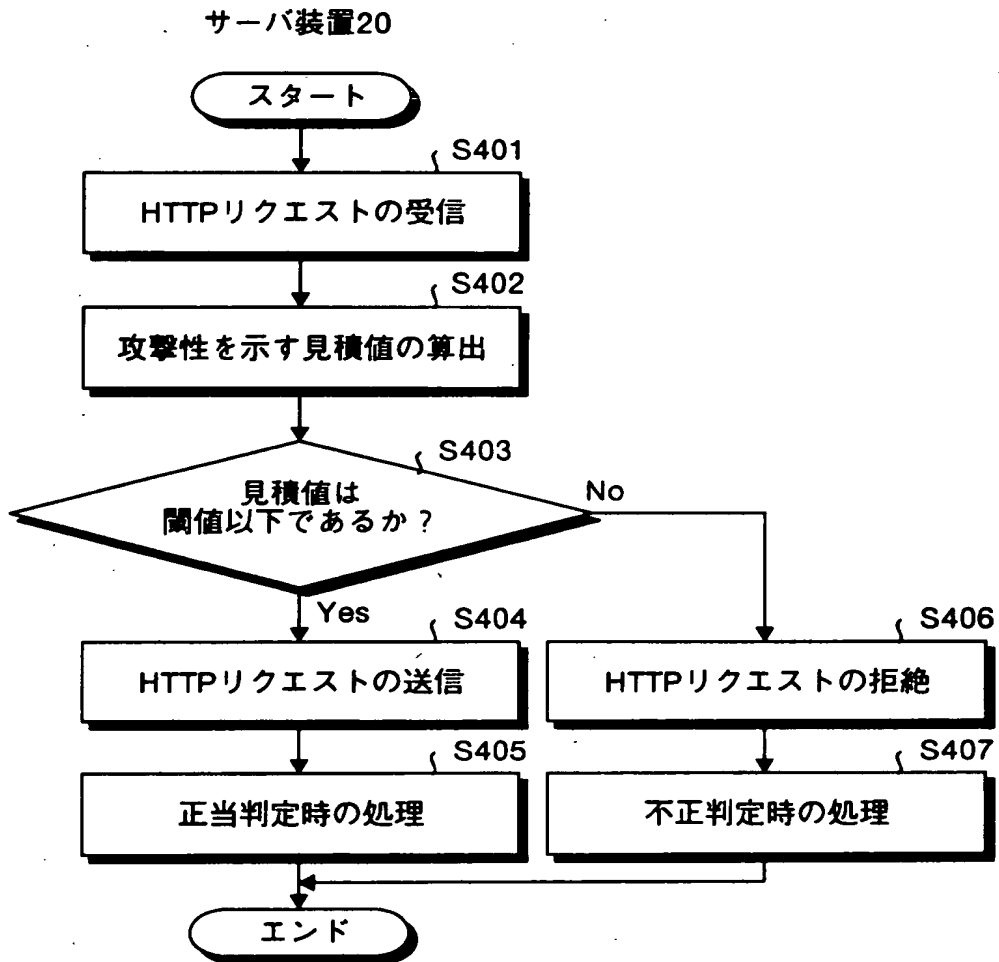
【図 3】

本実施の形態 1 によるフィルタリングの処理手順を示すフローチャート



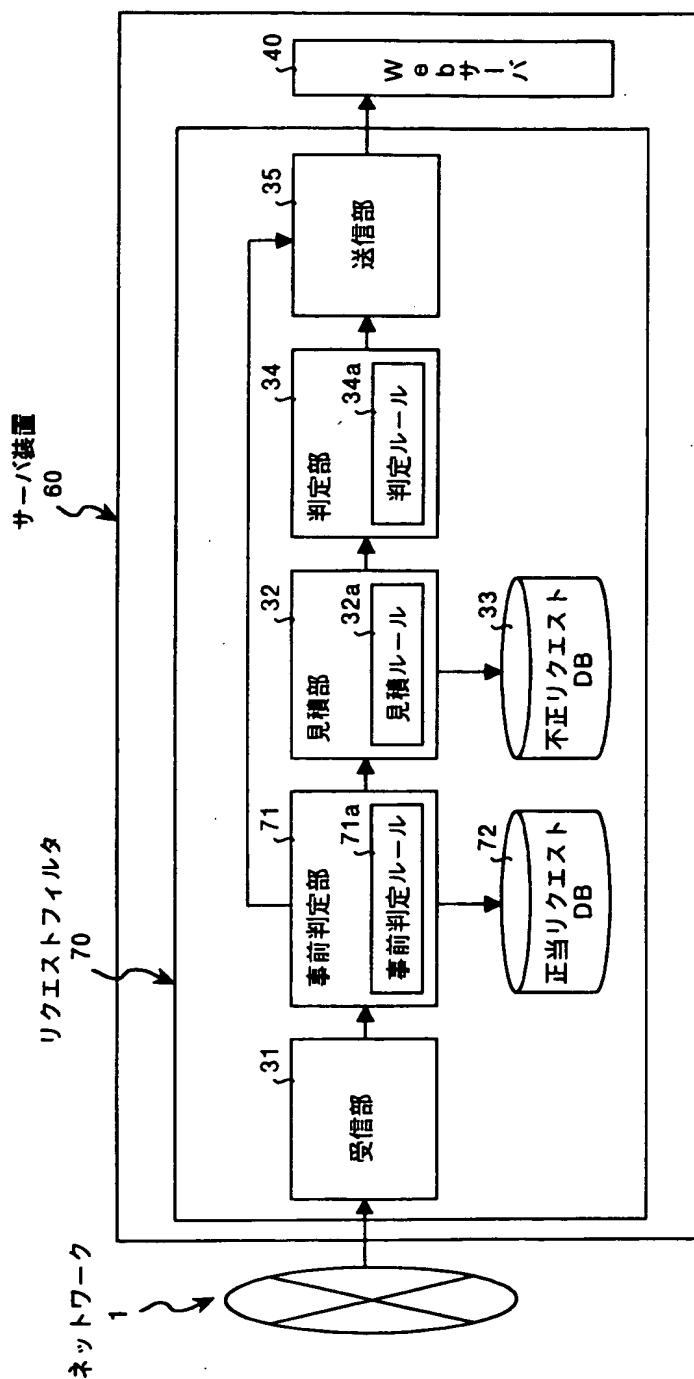
【図 4】

本実施の形態 2 によるフィルタリングの処理手順を示すフローチャート



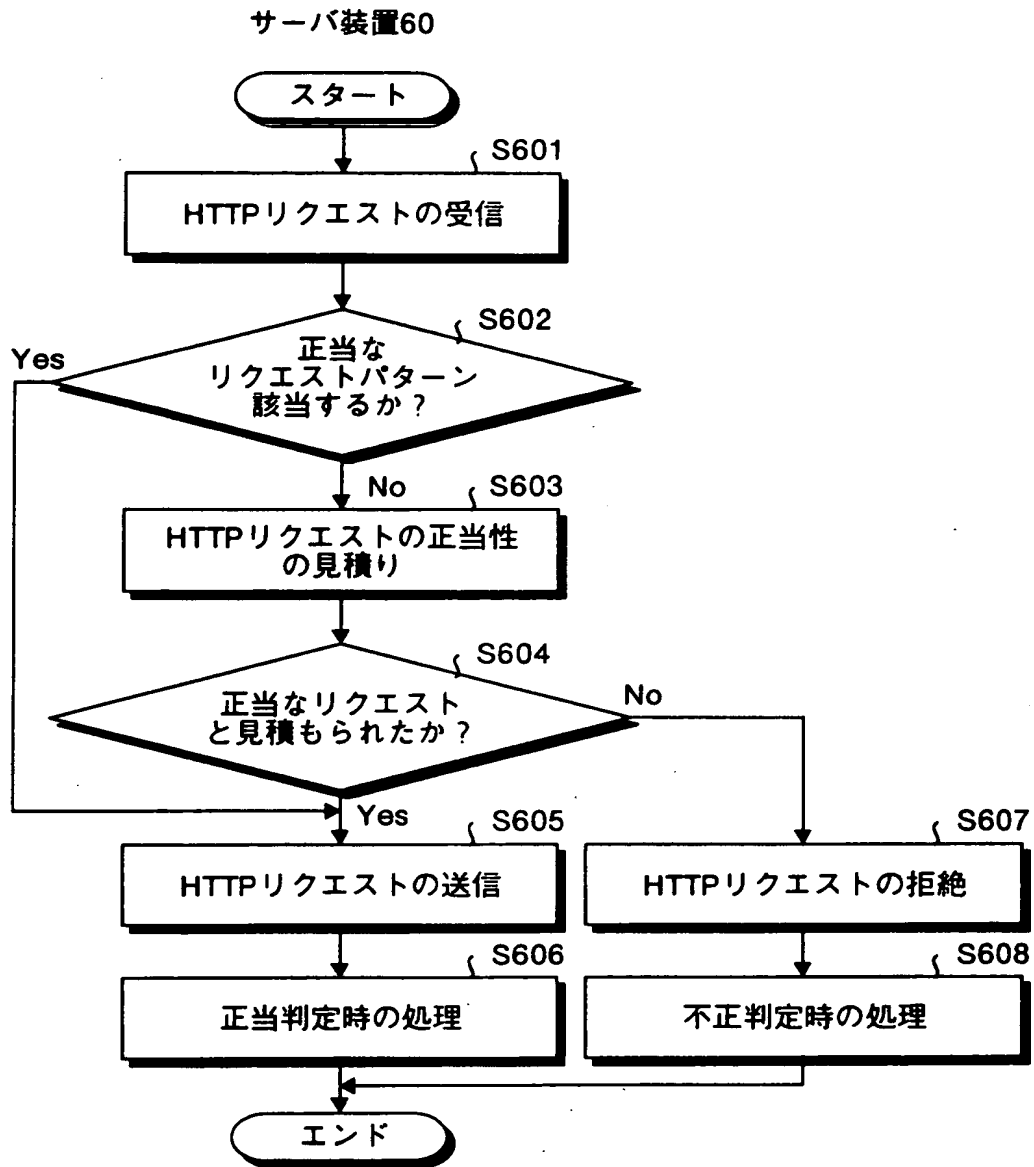
【図 5】

本実施の形態 3 に係るサーバクライアントシステムの構成を示すブロック図



【図 6】

本実施の形態 3 によるフィルタリングの処理手順を示すフローチャート



【書類名】 要約書

【要約】

【課題】 不正クライアントと認定されていないクライアントからの不正アクセスに対してもサーバを防御すること。

【解決手段】 Webサーバ40に対する不正アクセスのパターンを格納した不正リクエストDB（データベース）33と、不正リクエストDB33に格納された不正アクセスのパターンおよび所定の見積ルール32aに基づいてクライアント装置10からのアクセス要求の正当性を見積もる見積部32と、見積部32による見積結果および所定の判定ルール34aに基づいてアクセス要求をWebサーバ40に受け渡すか否かを判定する判定部34とを備える。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日
[変更理由] 住所変更
住 所 神奈川県川崎市中原区上小田中4丁目1番1号
氏 名 富士通株式会社